UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/706,728	11/07/2000	Patrick Le Quere	T2147-906625	8212

181 7590 05/07/2004

MILES & STOCKBRIDGE PC
1751 PINNACLE DRIVE
SUITE 500
MCLEAN, VA 22102-3833

EXAMINER	
COLIN, CARL G	

ART UNIT	PAPER NUMBER
2136	7

DATE MAILED: 05/07/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/706,728	LE QUERE, PATRICK	
	Examiner	Art Unit	
	Carl Colin	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *07 November 2000* .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *14-34* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *14-34* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *07 November 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) *5* .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

1. In response to preliminary amendment filed on 11/07/2000, paper 6, Applicant cancels claims 1-13 and adds claims 15-34. The amendments to the specification have been entered. Pursuant to USC 131, claims 14-34 are presented for examination.

Specification

2. The abstract of the disclosure is objected to because of the "means" language on line 8. Correction is required. See MPEP § 608.01(b).

Applicant is reminded of the proper language and format for an abstract of the disclosure.

The abstract should be in narrative form and generally limited to a single paragraph on a separate sheet within the range of 50 to 150 words. It is important that the abstract not exceed 150 words in length since the space provided for the abstract on the computer tape used by the printer is limited. The form and legal phraseology often used in patent claims, such as "means" and "said," should be avoided. The abstract should describe the disclosure sufficiently to assist readers in deciding whether there is a need for consulting the full patent text for details.

The language should be clear and concise and should not repeat information given in the title. It should avoid using phrases which can be implied, such as, "The disclosure concerns," "The disclosure defined by this invention," "The disclosure describes," etc.

2.1 The spacing of the lines of the specification is such as to make reading and entry of amendments difficult. New application papers with lines double spaced on good quality paper are required.

Claim Objections

3. **Claim 15 and the intervening claims** are objected to because of the following informalities: on lines 2 and 5, the phrase "the circuit (1)" is not consistent with "encryption circuit (1)". Also, on lines 4 and 11, the phrase "the host system (HS)" is not consistent with "host computer system". Line 8, the reference number should be placed after circuit. On line 11, "the parallelism" should be --a parallelism--. Appropriate correction is required to avoid rendering the claim indefinite.

3.1 **Claims 18-20** are objected to because of the following informalities: reference number (40) followed by "encryption algorithms" does not appear in the drawing. Claims 18-19, line 4, "the bus" should be replaced by --a first bus--.

3.2 **Claim 21** is objected to because of the following informalities: line 6, "to the" before the word "processing" should be corrected. On line 3, "the memory (4)" lacks consistency. On lines 2 and 9 " the encryption module (9)" is not consistent with "the encryption component (9)". Appropriate correction is required.

3.3 **Claim 22** is objected to because of the following informalities: line 2, "(30_" does not have a closed parenthesis and should be corrected. On line 3, "the memory (4)" lacks consistency. On lines 2 and 9 " the encryption module (9)" is not consistent with "the encryption component (9)". Appropriate correction is required.

3.4 **Claims 15, 17, 28, and 30** and the intervening claims are objected to because of the following informalities: in order to avoid rendering the claim indefinite, the term "adapted to" should be corrected. Appropriate correction is required.

3.4 Applicant's cooperation is requested in correcting any errors of which applicant may become aware in the application.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter, which the applicant regards as his invention.

Claims 14, 22-25 and the intervening claims are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

4.1 **Claim 14** is recites the limitation "Architecture according to claim 13" in the original claims filed on 11/07/2000. There is insufficient antecedent basis for this limitation in the claim.

4.2 Regarding **claims 22-25** the addition of the word "type" to an otherwise definite expression extends the scope of the expression so as to render it indefinite. See MPEP § 2173.05(e).

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

5.1 **Claims 15-17** and **30-32** are rejected under 35 U.S.C. 102(e) as being anticipated by US Patent 6,021,201 to **Bakhle et al.**.

5.2 **As per claim 15**, **Bakhle et al.** discloses an encryption circuit (1) for simultaneously processing various encryption algorithms, the circuit adapted to be coupled with a host computer system (HS), characterized in that the circuit comprises:

- an input/output module (2), for handling data exchanges between the host system (HS) and the circuit (1) via a dedicated bus (PCI), for example (see column 4, lines 26-67);

- an encryption module (3) coupled with the input/output module (2) said encryption module controlling encryption and decryption operations, as well as storage of all sensitive information (1) of the circuit, for example (see column 5, lines 1-26; column 6, lines 5-25; and column 4, lines 26-67); and

- isolation means (4) between the input/output module (2) and the encryption module (3), for making the sensitive information stored in the encryption module (3) inaccessible to the host system (HS) and for ensuring the parallelism of the operations performed by the input/output module (2) and the encryption module (3), for example (see column 4, lines 26-67).

As per claim 16, Bakhle et al. discloses an encryption circuit according to claim 15, characterized in that the isolation means (4) of the circuit (1) comprises a double-port memory (4), for example (see column 4, lines 26-67).

As per claim 17, Bakhle et al. discloses an encryption circuit according to claim 15 wherein this isolation means (4) comprises a double port memory coupled between the input/output module (2) and the encryption module (3), the dual-port memory (4) being coupled to a first bus and adapted to simultaneously handle the exchange of data, commands and statuses between the input/output and encryption modules (2 and 3), and isolation between the two modules (2 and 3), for example (see column 4, lines 26-67 and column 2, lines 43-54).

As per claim 30, Bakhle et al. shows that module 148 that includes the storage keys can be connected to a serial link, which is independent of the dedicated PCI bus that meets the

recitation of an encryption circuit according to claim 15 comprising a serial link (SL) connected to input basic keys through a secure path independent of the dedicated PCI bus, said link adapted to be controlled by the encryption module (3), for example (see column 12, line 48 through column 13, line 10).

As per claim 31, **Bakhle et al.** discloses the limitation of an encryption circuit according to claim 30, characterized in that the serial link (SL) allows downloading of proprietary algorithms into the first encryption sub-module (3_1), for example (see column 12, line 48 through column 13, line 10).

Claim 32 is similar to the rejected **claim 15** except for including a card to support the claimed circuit. Therefore, **claim 32** is rejected on the same rationale as the rejection of **claim 15**. **Bakhle et al.** discloses the claimed circuit of claim 15 and also discloses an apparatus that can be incorporated in any embodiment without departing from the spirit and the scope of the invention (see column 2, lines 40-65).

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have

been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6.1 **Claims 18-27, 29, and 33-34** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 6,021,201 to **Bakhle et al.** in view of IBM Technical Disclosure Bulletin, Cryptographic Microcode Loading Controller for Secure Function, September 1991, NB910934, Pages 1-5.

6.2 **As per claims 18-20, and 27, Bakhle et al.** discloses an encryption circuit is set forth in claim 15, characterized in that the encryption module (3) comprises:

- a first encryption sub-module (3_1), dedicated to the processing of symmetric encryption algorithms, and being coupled with the first bus of the dual port memory (4) , for example (see column 5, lines 14-67);

- a second encryption sub-module (3_2), dedicated to the processing of asymmetric encryption algorithms (40) and being coupled with the first bus of the dual-port memory (4) and including a separate internal second bus isolated from the first bus of the dual-port memory (4), for example (see column 5, lines 14-67 and see figure 3); and

Bakhle et al. discloses a RAM memory storing the encryption keys and coupled with the bus of the dual port memory (see figures 1-3) that meets the recitation of a CMOS memory (11) coupled with the dual-port memory (4) via the first bus of the dual-port memory containing the encryption keys, for example (see column 6, lines 5-21), which is well known in the art.

Bakhle et al. does not explicitly disclose an additional flash memory in the second encryption sub-module in claim 27 or stating specifically using a CMOS in claims 18-20 and 28. These elements are well known in the art in a security device and can be implemented by the invention disclosed in the reference as mentioned above. IBM Technical Disclosure Bulletin supports well known art by disclosing a single-chip microcontroller comprising flash memory, data RAM memory, CMOS memory; the flash memory. This bulletin further uses a CMOS memory to store security keys because it has the advantage to make probing and examination more difficult in attempt of removal as the CMOS's is sensitive to light and static charge. In addition the RAMs could be backed with a battery when the system was unpowered. Therefore, it would have been obvious to one of ordinary skill in the art of computer security at the time the invention was made to modify the circuit of **Bakhle et al.** to provide an additional flash memory in the second encryption sub-module or provide a CMOS memory as taught by IBM Technical Disclosure Bulletin. This modification would have been obvious because one skilled in the art would have been motivated to do so in order to make probing and examination more difficult in attempt of removal and the other advantage would be that the RAMs could be backed with a battery when the system was unpowered.

As per claim 21, **Bakhle et al.** discloses the limitation of an encryption circuit characterized in that the first encryption sub-module (3_1) comprises an encryption component (9) coupled with the dual-port memory (4) via the first bus of the memory (4), comprising various encryption automata, respectively dedicated to the processing of symmetric encryption algorithms, and in that the second encryption sub-module (3_1) comprises at least two encryption

processors (10_1 and 10_2), respectively dedicated to the processing of asymmetric encryption algorithms, coupled with the encryption module (9) via the internal second bus of the second sub-module (3_2), for example (see column 5, lines 14-67 and see figures 3 and 6 with description); and discloses a control unit comprises a security unit that control input and output and use buses separating from the dual port bus (see figures 3-6 with description and table 2, column 8; column 13, lines 10 et seq.) that meets the recitation of and a bus isolator (14) for isolating the second bus from the first bus of the dual port memory. **Bakhle et al.** discloses that the cipher and the hash unit can be implemented with specific dedicated hardware components known in the art for processing of asymmetric and symmetric algorithms (see end of column 5).

As per claims 22-23, and 25, Bakhle et al. discloses the limitation of an encryption circuit characterized in that one (10_1) of the two encryption processors (10_1 and 10_2) is of the CIP type, and in that the other (10_2) of the two encryption processors is of the ACE type, for example (see column 5, lines 50-67). **Bakhle et al.** discloses that the cipher and the hash unit can be implemented with specific dedicated hardware components known in the art for processing of asymmetric and symmetric algorithms (see end of column 5). Having both processors CIP type is a design choice.

As per claims 24 and 26, Bakhle et al. does not explicitly disclose that one of the processors and the encryption component comprise a FPGA. **Bakhle et al.** discloses input output buffer arrays, for example (see column 9, lines 55 et seq.) and also discloses that the cipher and the hash unit can be implemented with specific dedicated hardware components

known in the art for processing of asymmetric and symmetric algorithms (see end of column 5). It is apparent to one skilled in the art that the units disclosed by **Bakhle et al.** can comprise FPGA without departing from the spirit and scope of the invention as such unit and component are also well known in the art.

As per claim 29, **Bakhle et al.** substantially disclose the limitation of an encryption circuit according to claim 15 characterized in that the input/output module (2) comprises: a microcontroller (6) having an input/output processor (6_1) and a PCI interface (6_2) integrating DMA channels responsible for executing the data transfers between the host system (HS) and the circuit (1), for example (see column 4, lines 26-67 and column 5, lines 34-44);

- a flash memory (7) containing the code of the input/output processor (6_1) and a PCI interface (6_2), integrating DMA channels responsible for executing the data transfers between the host system (HS) and the circuit (1), for example (see column 4, lines 26-67);
- a flash memory (7) containing the code of the input/output processor (6_1), for example (see column 4, lines 38-42); and
- an SRAM memory (8) that receives a copy of the contents of the flash memory (7) upon startup of the input/output processor (6_2), for example (see column 4, lines 26-67). **Bakhle et al.** discloses instructions in the memory subsystem for the processors and examples of memory devices and the like that can be implemented with the I/O module, such examples include DRAM, ROM, VRAM and the like. It is apparent to one skilled in the art that any modifications of ROM or RAM memory used such as a flash memory or SRAM will not depart from the spirit and scope of the invention disclosed by **Bakhle et al.** as it is well known in the art.

Claim 33 is similar to the rejected **claim 18** except for including a card to support the claimed circuit. Therefore, **claim 32** is rejected on the same rationale as the rejection of **claim 18**. **Bakhle et al.** discloses the claimed circuit of claim 18 and also discloses an apparatus that can be incorporated in any embodiment without departing from the spirit and the scope of the invention (see column 2, lines 40-65).

Claim 34 is similar to the rejected **claim 21** except for including a card to support the claimed circuit. Therefore, **claim 32** is rejected on the same rationale as the rejection of **claim 21**. **Bakhle et al.** discloses the claimed circuit of claim 21 and also discloses an apparatus that can be incorporated in any embodiment without departing from the spirit and the scope of the invention (see column 2, lines 40-65).

7. **Claim 28** is rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 6,021,201 to **Bakhle et al.** in view of IBM Technical Disclosure Bulletin, Cryptographic Microcode Loading Controller for Secure Function, September 1991, NB910934, Pages 1-5 as applied to claims 18-27 above, and further in view of US Patent 5,682,027 to **Bertina et al.**.

7.1 **As per claim 28,** both references substantially teach the claimed circuit of claim 21 and a CMOS memory containing security keys. Neither of the references explicitly teaches a security mechanism to trigger a reset mechanism. **Bertina et al.** in an analogous art discloses program stored in a mask ROM that can execute at power on to provide a security mechanism for

unlocking a circuit card after too many wrong passwords and possibly encryption (see column 2, lines 19-32). Therefore, it would have been obvious to one of ordinary skill in the art of computer security at the time the invention was made to modify the circuit of **Bakhle et al.** to provide a security mechanism adapted to trigger a reset mechanism to the CMOS memory as taught by **Bertina et al.**. This modification would have been obvious because one skilled in the art would have been motivated by the suggestions provided by **Bertina et al.** so as to unlock a circuit card after too many wrong passwords and possibly encryption.

Conclusion

8. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure as the first art discloses parallel and processing system and method and the second art discloses manipulation of processing operations by an agent connected to dedicated memory.

US Patents:	6,079,008	Clery, III
	6,357,004	Davis

8.1 Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carl Colin whose telephone number is 703-305-0355. The examiner can normally be reached on Monday through Thursday, 8:00-6:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

ce

Carl Colin

Patent Examiner

April 29, 2004

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100